On Random Linear Network Coding for Butterfly Network

Xuan Guang, and Fang-Wei Fu

Abstract—**Random linear network coding is a feasible encoding tool for network coding, specially for the non-coherent network, and its performance is important in theory and application. In this letter, we study the performance of random linear network coding for the well-known butterfly network by analyzing the failure probabilities. We determine the failure probabilities of random linear network coding for the well-known butterfly network and the butterfly network with channel failure probability p.**

Index Terms—**Network coding, random linear network coding, butterfly network, failure probabilities.**

I. INTRODUCTION

IN the seminal paper [1], Ahlswede *et al* showed that with network coding, the source node can multicast information to all sink nodes at the theoretically maximum rate as the alphabet size approaches infinity, where the theoretically maximum rate is the smallest minimum cut capacity between the source node and any sink node. Li *et al* [2] showed that linear network coding with finite alphabet is sufficient for multicast. Moreover, the well-known butterfly network was proposed in papers [1] [2] to show the advantages of network coding well compared with routing. Koetter and Médard [3] presented an algebraic characterization of network coding. Ho *et al* [4] proposed the random linear network coding and gave several upper bounds on the failure probabilities of random linear network coding. Balli, Yan, and Zhang [5] improved on these bounds and discussed the limit behavior of the failure probability as the field size goes to infinity.

In this paper, we study the failure probabilities of random linear network coding for the well-known butterfly network when it is considered as a single source multicast network described by Fig. 1, and discuss the limit behaviors of the failure probabilities as the field size goes to infinity.

II. FAILURE PROBABILITIES OF RANDOM LINEAR NETWORK CODING FOR BUTTERFLY NETWORK

In this letter, we always denote $G = (V, E)$ the butterfly network shown by Fig. 1, where the single source node is s, the set of sink nodes is $T = \{t_1, t_2\}$, the set of internal nodes is $J = \{s_1, s_2, i, j\}$, and the set of the channels is $E = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9\}$. Moreover, we assume that each channel $e \in E$ is error-free, and the capacity is unit
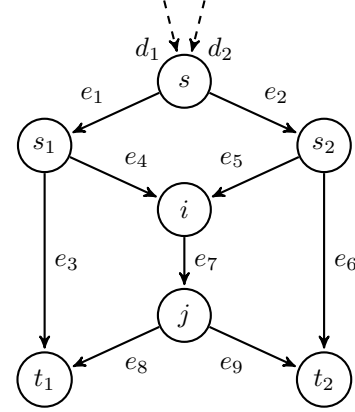
Fig. 1. Butterfly Network where d_1, d_2 represent two imaginary incoming channels of source node s.

1. It is obvious that both values of the maximum flows for the sink nodes t_1 and t_2 are 2.

Now we consider random linear network coding problem with the information rate 2 for this butterfly network G. That is to say, for source node s and internal nodes, all local encoding coefficients are independently uniformly distributed random variables taking values in the base field $\mathcal{F}$. For source node s, although it has no incoming channels, we use two imaginary incoming channels d_1, d_2 and assume that they provide the source messages for s. Let the global encoding kernels of $f_{d_1} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $f_{d_2} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, respectively. The local encoding kernel at the source node s is denoted as $K_s = \begin{pmatrix} k_{d_1,1} & d_{d_1,2} \\ k_{d_2,1} & d_{d_2,2} \end{pmatrix}$.

Similarly, we denote by f_i the global encoding kernel of channel e_i $(1 \leq i \leq 9)$, and $k_{i,j}$ the local encoding coefficient for the pair (e_i, e_j) with $head(e_i) = tail(e_j)$ as described in [6, p.442], where $tail(e_i)$ represents the node whose outgoing channels include e_i, $head(e_i)$ represents the node whose incoming channels include e_i:

$$f_1 = k_{d_1,1}f_{d_1} + k_{d_2,1}f_{d_2} = \begin{pmatrix} k_{d_1,1} \\ k_{d_2,1} \end{pmatrix},$$

$$f_2 = k_{d_1,2}f_{d_1} + k_{d_2,2}f_{d_2} = \begin{pmatrix} k_{d_1,2} \\ k_{d_2,2} \end{pmatrix},$$

$$f_3 = k_{1,3}f_1 = \begin{pmatrix} k_{d_1,1}k_{1,3} \\ k_{d_2,1}k_{1,3} \end{pmatrix}, f_4 = k_{1,4}f_1 = \begin{pmatrix} k_{d_1,1}k_{1,4} \\ k_{d_2,1}k_{1,4} \end{pmatrix},$$

$$f_5 = k_{2,5}f_2 = \begin{pmatrix} k_{d_1,2}k_{2,5} \\ k_{d_2,2}k_{2,5} \end{pmatrix}, f_6 = k_{2,6}f_2 = \begin{pmatrix} k_{d_1,2}k_{2,6} \\ k_{d_2,2}k_{2,6} \end{pmatrix},$$

$$f_7 = k_{4,7}f_4 + k_{5,7}f_5 = \begin{pmatrix} k_{d_1,1}k_{1,4}k_{4,7} + k_{d_1,2}k_{2,5}k_{5,7} \\ k_{d_2,1}k_{1,4}k_{4,7} + k_{d_2,2}k_{2,5}k_{5,7} \end{pmatrix},$$

$$f_8 = k_{7,8}f_7 = \begin{pmatrix} k_{d_1,1}k_{1,4}k_{4,7}k_{7,8} + k_{d_1,2}k_{2,5}k_{5,7}k_{7,8} \\ k_{d_2,1}k_{1,4}k_{4,7}k_{7,8} + k_{d_2,2}k_{2,5}k_{5,7}k_{7,8} \end{pmatrix},$$

$$f_9 = k_{7,9}f_7 = \begin{pmatrix} k_{d_1,1}k_{1,4}k_{4,7}k_{7,9} + k_{d_1,2}k_{2,5}k_{5,7}k_{7,9} \\ k_{d_2,1}k_{1,4}k_{4,7}k_{7,9} + k_{d_2,2}k_{2,5}k_{5,7}k_{7,9} \end{pmatrix}$$

and the decoding matrices of the sink nodes t_1, t_2 are

$$F_{t_1} = \begin{pmatrix} k_{d_1,1}k_{1,3} & k_{d_1,1}k_{1,4}k_{4,7}k_{7,8} + k_{d_1,2}k_{2,5}k_{5,7}k_{7,8} \\ k_{d_2,1}k_{1,3} & k_{d_2,1}k_{1,4}k_{4,7}k_{7,8} + k_{d_2,2}k_{2,5}k_{5,7}k_{7,8} \end{pmatrix}, \tag{1}$$

$$F_{t_2} = \begin{pmatrix} k_{d_1,2}k_{2,6} & k_{d_1,1}k_{1,4}k_{4,7}k_{7,9} + k_{d_1,2}k_{2,5}k_{5,7}k_{7,9} \\ k_{d_2,2}k_{2,6} & k_{d_2,1}k_{1,4}k_{4,7}k_{7,9} + k_{d_2,2}k_{2,5}k_{5,7}k_{7,9} \end{pmatrix}. \tag{2}$$

A. Butterfly Network without Fail Channels

Next, we begin to discuss the failure probabilities of random linear network coding for the butterfly network G. These failure probabilities can illustrate the performance of the random linear network coding for the butterfly network. First, we give the definitions of failure probabilities.

Definition 1: For random linear network coding for the butterfly network G with information rate 2:

- $P_e(t_i) \triangleq Pr(\text{Rank}(F_{t_i}) < 2)$ is called the failure probability of sink node t_i, that is the probability that the messages cannot be decoded correctly at t_i $(i = 1, 2)$;
- $P_e \triangleq Pr(\exists\, t \in T \text{ such that Rank}(F_t) < 2)$ is called the failure probability of the butterfly network G, that is the probability that the messages cannot be decoded correctly at at least one sink node in T;
- $P_{av} \triangleq \frac{\sum_{t \in T} P_e(t)}{|T|}$ is called the average failure probability of all sink nodes for the butterfly network G.

To determine the failure probabilities of random linear network coding for the butterfly network G, we need the following lemma.

Lemma 1: Let M be a uniformly distributed random 2×2 matrix over a finite field $\mathcal{F}$, then the probability that M is invertible is $(|\mathcal{F}| + 1)(|\mathcal{F}| - 1)^2/|\mathcal{F}|^3$.

Theorem 1: For random linear network coding for the butterfly network G with information rate 2:

- the failure probability of the sink node t_i $(i = 1, 2)$ is

$$P_e(t_i) = 1 - \frac{(|\mathcal{F}| + 1)(|\mathcal{F}| - 1)^6}{|\mathcal{F}|^7} ;$$

- the failure probability of the butterfly network G is

$$P_e = 1 - \frac{(|\mathcal{F}| + 1)(|\mathcal{F}| - 1)^{10}}{|\mathcal{F}|^{11}} ;$$

- the average failure probability is

$$P_{av} = 1 - \frac{(|\mathcal{F}| + 1)(|\mathcal{F}| - 1)^6}{|\mathcal{F}|^7} .$$

Proof: Recall that $K_s = (f_1\ f_2)$ is the local encoding kernel at the source node s. Denote

$$B_1 \triangleq \begin{pmatrix} k_{1,3} & k_{1,4}k_{4,7}k_{7,8} \\ 0 & k_{2,5}k_{5,7}k_{7,8} \end{pmatrix}, B_2 \triangleq \begin{pmatrix} 0 & k_{1,4}k_{4,7}k_{7,9} \\ k_{2,6} & k_{2,5}k_{5,7}k_{7,9} \end{pmatrix}.$$

Then, we know from (1) and (2) that $F_{t_1} = K_s B_1$, $F_{t_2} = K_s B_2$. Moreover, from Lemma 1, we have

$$\begin{aligned} 1 - P_e(t_1) &= Pr(\text{Rank}(F_{t_1}) = 2) = Pr(\det(F_{t_1}) \neq 0) \\ &= Pr(\{\det(K_s) \neq 0\} \cap \{\det(B_1) \neq 0\}) \\ &= Pr(\det(K_s) \neq 0) \cdot Pr(\det(B_1) \neq 0) \\ &= \frac{(|\mathcal{F}| + 1)(|\mathcal{F}| - 1)^2}{|\mathcal{F}|^3} \left(\frac{|\mathcal{F}| - 1}{|\mathcal{F}|}\right)^4 \\ &= \frac{(|\mathcal{F}| + 1)(|\mathcal{F}| - 1)^6}{|\mathcal{F}|^7}. \end{aligned}$$

Similarly, we also have $1 - P_e(t_2) = (|\mathcal{F}| + 1)(|\mathcal{F}| - 1)^6/|\mathcal{F}|^7$.

Next, we consider the failure probability P_e. Similar to the above analysis, we have

$$\begin{aligned} 1 - P_e &= Pr(\{\text{Rank}(F_{t_1}) = 2\} \cap \{\text{Rank}(F_{t_2}) = 2\}) \\ &= Pr(\{\det(F_{t_1}) \neq 0\} \cap \{\det(F_{t_2}) \neq 0\}) \\ &= Pr(\{\det(K_s) \neq 0\} \cap \{\det(B_1) \neq 0\} \cap \{\det(B_2) \neq 0\}) \\ &= Pr(\det(K_s) \neq 0) \cdot Pr(\det(B_1) \neq 0) \cdot Pr(\det(B_2) \neq 0) \\ &= \frac{(|\mathcal{F}| + 1)(|\mathcal{F}| - 1)^{10}}{|\mathcal{F}|^{11}}. \end{aligned}$$

Moreover, since $P_{av} = \frac{P_e(t_1) + P_e(t_2)}{2}$, then we have

$$P_{av} = 1 - \frac{(|\mathcal{F}| + 1)(|\mathcal{F}| - 1)^6}{|\mathcal{F}|^7} .$$

This completes the proof. ∎

It is known that if $|\mathcal{F}| \geq |T|$, there exists a linear network code $\mathbf{C}$ such that all sink nodes can decode successfully $w = \min_{t \in T} C_t$ symbols generated by the source node s, where C_t is the minimum cut capacity between s and the sink node t. For butterfly network, $|\mathcal{F}| \geq 2$ is enough. However, when we consider the performance of random linear network coding, the result is different.

For $|\mathcal{F}| = 2$, we have $1 - P_e = \frac{3}{2^{11}} \approx 0.001$. In other words, this successful probability is too much low for application. In the same way, for $|\mathcal{F}| = 3$ and $|\mathcal{F}| = 4$, the successful probabilities are approximately 0.023 and 0.070, respectively. These successful probabilities are still too low for application.

If $1 - P_e \geq 0.9$ is thought of enough for application, we have to choose a very large base field $\mathcal{F}$ with cardinality not less than 87. This is because

$$\frac{(|\mathcal{F}| + 1)(|\mathcal{F}| - 1)^{10}}{|\mathcal{F}|^{11}} \geq 0.9 \Longleftrightarrow |\mathcal{F}| \geq 87 .$$

B. Butterfly Network with Fail Channels

In this subsection, as in [4], we will consider the failure probabilities of random linear network coding for the butterfly network with channel failure probability p (i.e., each channel is possibly deleted from the network with probability p). Generally speaking, channel failure is a low probability event, i.e., $0 \leq p \ll \frac{1}{2}$. In fact, if $p = 0$, it is just the butterfly network without fail channels discussed in the above subsection.

Theorem 2: For the random linear network coding of the butterfly network G with channel failure probability p,

- the failure probability of the sink node t_i $(i = 1, 2)$ is

$$\tilde{P}_e(t_i) = 1 - \frac{(|\mathcal{F}| + 1)(|\mathcal{F}| - 1)^6}{|\mathcal{F}|^7}(1 - p)^6 \; ;$$

- the failure probability of the butterfly network G is

$$\tilde{P}_e = 1 - \frac{(|\mathcal{F}| + 1)(|\mathcal{F}| - 1)^{10}}{|\mathcal{F}|^{11}}(1 - p)^9 \; ;$$

- the average failure probability is

$$\tilde{P}_{av} = 1 - \frac{(|\mathcal{F}| + 1)(|\mathcal{F}| - 1)^6}{|\mathcal{F}|^7}(1 - p)^6 \; .$$

Proof: At first, we consider the failure probability $\tilde{P}_e(t_1)$. For each channel e_i, we call "channel e_i is successful" if e_i is not deleted from the network, and define δ_i as the event that "e_i is successful". We define $\tilde{f}_i$ as the *active global encoding kernel* of e_i, where

$$\tilde{f}_i = \begin{cases} f_i, & e_i \text{ is successful,} \\ \underline{0}, & \text{otherwise.} \end{cases}$$

and $f_i = \sum_{j:head(e_j)=tail(e_i)} k_{j,i}\tilde{f}_j$. Then the decoding matrix of the sink node t_1 is $F_{t_1} = (\tilde{f}_3 \; \tilde{f}_8)$. Hence, $\tilde{P}_e(t_1) = Pr(\text{Rank}((\tilde{f}_3 \; \tilde{f}_8)) \neq 2)$.

Note that the event "$\text{Rank}((\tilde{f}_3 \; \tilde{f}_8)) = 2$" is equivalent to the event "$\text{Rank}((f_3 \; f_8)) = 2$, δ_3, and δ_8". Moreover, since $(f_3 \; f_8) = (k_{1,3}f_1 \; k_{7,8}f_7)$, we have $\text{Rank}((f_3 \; f_8)) = 2$ if and only if $\text{Rank}((\tilde{f}_1 \; \tilde{f}_7)) = 2$ and $k_{1,3} \neq 0, k_{7,8} \neq 0$. Similarly, the event "$\text{Rank}((\tilde{f}_1 \; \tilde{f}_7)) = 2$" is equivalent to the event "$\text{Rank}((f_1 \; f_7)) = 2$, δ_1, and δ_7". Note that $\tilde{f}_4 = \underline{0}$ or f_4, and $f_4 = k_{1,4}f_1$, so $\tilde{f}_4 = \underline{0}$ or $k_{1,4}f_1$. Since $f_7 = k_{4,7}\tilde{f}_4 + k_{5,7}\tilde{f}_5$, we have $\text{Rank}((f_1 \; f_7)) = 2$ if and only if $\text{Rank}((f_1 \; \tilde{f}_5)) = 2$ and $k_{5,7} \neq 0$. Going on with the same analysis as above, we have that the event "$\text{Rank}((f_1 \; \tilde{f}_5)) = 2$" is equivalent to the event "$\text{Rank}((f_1 \; f_5)) = 2$, and δ_5", and the event "$\text{Rank}((f_1 \; f_5)) = 2$" is equivalent to the event "$\text{Rank}((f_1 \; f_2)) = 2$, $k_{2,5} \neq 0$, and δ_2" since $f_5 = k_{2,5}f_2$. Therefore, the event "$\text{Rank}((\tilde{f}_3 \; \tilde{f}_8)) = 2$" is equivalent to the event "$\text{Rank}((f_1 \; f_2)) = 2$, δ_1, δ_2, δ_3, δ_5, δ_7, δ_8, and $k_{1,3}, k_{2,5}, k_{5,7}, k_{7,8} \neq 0$". Hence, we have

$$1 - \tilde{P}_e(t_1) = Pr(\text{Rank}((\tilde{f}_3 \; \tilde{f}_8)) = 2)$$
$$= Pr(\{\text{Rank}(f_1 \; f_2) = 2\} \cap \{\delta_1, \delta_2, \delta_3, \delta_5, \delta_7, \delta_8\}$$
$$\cap \{k_{1,3}, k_{2,5}, k_{5,7}, k_{7,8} \neq 0\})$$
$$= Pr(\{\text{Rank}(f_1 \; f_2) = 2\}) \cdot Pr(\{\delta_1, \delta_2, \delta_3, \delta_5, \delta_7, \delta_8\})$$
$$\cdot Pr(\{k_{1,3}, k_{2,5}, k_{5,7}, k_{7,8} \neq 0\})$$
$$= \frac{(|\mathcal{F}| + 1)(|\mathcal{F}| - 1)^6}{|\mathcal{F}|^7}(1 - p)^6.$$

In the same way, we can get

$$\tilde{P}_e(t_2) = \tilde{P}_e(t_1) = 1 - \frac{(|\mathcal{F}| + 1)(|\mathcal{F}| - 1)^6}{|\mathcal{F}|^7}(1 - p)^6 \; .$$

For the failure probability $\tilde{P}_e$, with the same analysis as above, we have

$$1 - \tilde{P}_e = Pr(\{\text{Rank}(F_{t_1}) = 2\} \cap \{\text{Rank}(F_{t_2}) = 2\})$$
$$= Pr(\{\text{Rank}((\tilde{f}_3 \; \tilde{f}_8)) = 2\} \cap \{\text{Rank}((\tilde{f}_6 \; \tilde{f}_9)) = 2\})$$

$$= Pr(\{\text{Rank}((f_1 \; f_2)) = 2\} \cap \{\delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6, \delta_7, \delta_8, \delta_9\}$$
$$\cap \{k_{1,3}, k_{2,5}, k_{5,7}, k_{7,8}, k_{2,6}, k_{1,4}, k_{4,7}, k_{7,9} \neq 0\})$$
$$= Pr(\text{Rank}((f_1 \; f_2)) = 2) \cdot Pr(\delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6, \delta_7, \delta_8, \delta_9)$$
$$\cdot Pr(\{k_{1,3}, k_{2,5}, k_{5,7}, k_{7,8}, k_{2,6}, k_{1,4}, k_{4,7}, k_{7,9} \neq 0\})$$
$$= \frac{(|\mathcal{F}| + 1)(|\mathcal{F}| - 1)^{10}}{|\mathcal{F}|^{11}}(1 - p)^9.$$

At last, the average probability $\tilde{P}_{av}$ is given by

$$\tilde{P}_{av} = \frac{\tilde{P}_e(t_1) + \tilde{P}_e(t_2)}{2} = 1 - \frac{(|\mathcal{F}| + 1)(|\mathcal{F}| - 1)^6}{|\mathcal{F}|^7}(1 - p)^6 \; .$$

The proof is completed. ∎

III. THE LIMIT BEHAVIORS OF THE FAILURE PROBABILITIES

In this section, we will discuss the limit behaviors of the failure probabilities. From Theorem 2, we have

$$\lim_{|\mathcal{F}| \to \infty} \tilde{P}_e(t_i) = \lim_{|\mathcal{F}| \to \infty} \tilde{P}_{av} = 1 - (1 - p)^6 \; , (i = 1, 2) \; ,$$
$$\lim_{|\mathcal{F}| \to \infty} \tilde{P}_e = 1 - (1 - p)^9 \; .$$

Specially, if we consider the random linear network coding for the butterfly network without fail channels, i.e. $p = 0$, we have (also from Theorem 1)

$$\lim_{|\mathcal{F}| \to \infty} P_e(t_i) = \lim_{|\mathcal{F}| \to \infty} P_e = \lim_{|\mathcal{F}| \to \infty} P_{av} = 0 \; , \; (i = 1, 2).$$

That is, for the sufficient large base field $\mathcal{F}$, the failure probabilities can become arbitrary small. In fact, this result is correct for all single source multicast network coding [4]. It is easy to see from Theorem 1 that the rates of $P_e(t_i)$ approaching 0 and P_{av} approaching 0 are $\frac{5}{|\mathcal{F}|}$, and the rate of P_e approaching 0 is $\frac{9}{|\mathcal{F}|}$.

IV. CONCLUSION

The performance of random linear network coding is illustrated by the failure probabilities of random linear network coding. In general, it is very difficult to calculate the failure probabilities of random linear network coding for a general communication network. In this letter, we determine the failure probabilities of random linear network coding for the well-known butterfly network and the butterfly network with channel failure probability p.

REFERENCES

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network Information Flow," IEEE Transactions on Information Theory, vol. 46, no. 4, pp. 1204-1216, Jul. 2000.
[2] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear Network Coding," IEEE Transactions on Information Theory, vol. 49, no. 2, pp. 371-381, Jul. 2003.
[3] R. Koetter, and M. Médard, "An Algebraic Approach to Network Coding," IEEE/ACM Transactions on Networking, vol. 11, no. 5, pp. 782-795, Oct. 2003.
[4] T. Ho, R. Koetter, M. Médard, M. Effors, J. Shi, and D. Karger, "A Random Network Coding Approach to Multicast," IEEE Transactions on Information Theory, vol. 52, no. 10, pp. 4413-4430, Jul. 2006.
[5] H. Balli, X. Yan, and Z. Zhang, "On Randomized Linear Network Codes and Their Error Correction Capabilities," IEEE Transactions on Information Theory, vol. 55, no. 7, pp. 3148-3160, Jul. 2009.
[6] R. W. Yeung, "Information Theory and Network Coding," Springer 2008.